

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

THIS PAGE BLANK (USPTO)

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000137681 A

(43) Date of publication of application: 16 . 05 . 00

(51) Int. Cl. G06F 15/00
G06F 19/00
G09C 1/00
H04L 9/32

(21) Application number: 10310686

(71) Applicant: TOSHIBA CORP

(22) Date of filing: 30 . 10 . 98

(72) Inventor: SHIMIZU MAKOTO

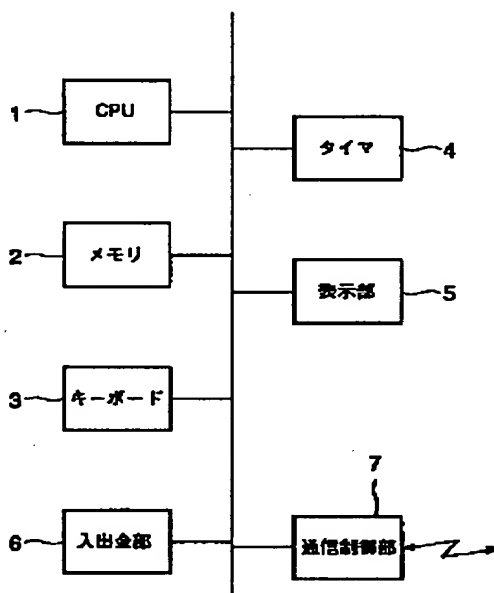
(54) INDIVIDUAL AUTHENTICATION METHOD AND
DEVICE

COPYRIGHT: (C)2000,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an individual authentication method and device capable of preventing illegal use due to impersonation into the person himself, and improving the precision of individual authentication.

SOLUTION: A character input interval at the time of the password data input of a person to be authenticated is preliminarily registered. When the person to be authenticated inputs the password data, the character input interval is measured, and collated with the preliminarily registered character input terminal, and when the inputted password data is coincident with the registered password data, and the measured character input interval is coincident with the registered character input interval within the range of a preliminarily set allowable error value, it is authenticated that the person to be authenticated is the person himself.



THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2000-137681

(P 2000-137681A)

(43) 公開日 平成12年5月16日 (2000. 5. 16)

(51) Int. Cl. ⁷	識別記号	F I	テーマ* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 B	5B055
	19/00	G 0 9 C 1/00 6 4 0 A	5B085
G 0 9 C 1/00	6 4 0	G 0 6 F 15/30 3 4 0	5J104
H 0 4 L 9/32		H 0 4 L 9/00 6 7 3 A	9A001
		6 7 5 A	
審査請求 未請求 請求項の数 16		O L	(全 15 頁)

(21) 出願番号 特願平10-310686

(22) 出願日 平成10年10月30日 (1998. 10. 30)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 清水 眞

神奈川県川崎市幸区柳町70番地 株式会社

東芝柳町工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

F ターム (参考) 5B055 BB10 HA04 HA17 HB01

5B085 AE03 AE15 AE23 AE29

5J104 AA07 KA01 KA04 KA14 NA05

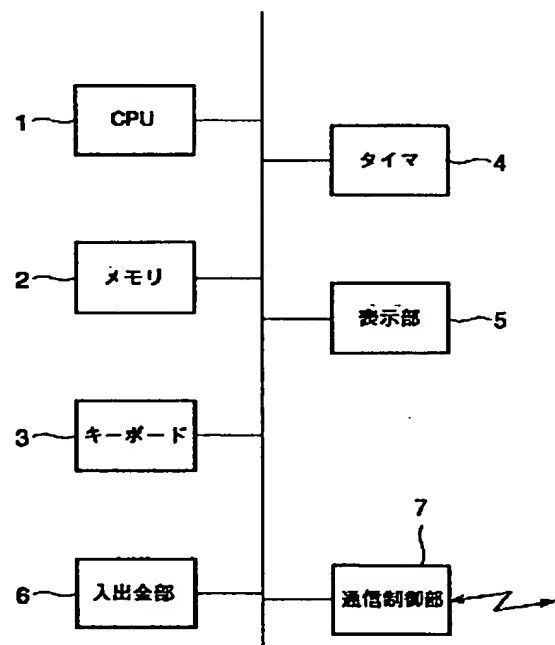
9A001 JJ58 JJ65 LL03

(54) 【発明の名称】 個人認証方法および個人認証装置

(57) 【要約】

【課題】 本人へのなりすましによる不正使用を防止でき、個人認証の精度が著しく向上する個人認証方法および個人認証装置を提供する。

【解決手段】 被認証者のパスワードデータ入力時における文字入力間隔をあらかじめ登録しておき、被認証者が行なうパスワードデータ入力の際にその文字入力間隔をそれぞれ計測して、あらかじめ登録された文字入力間隔と照合することにより、入力されたパスワードデータと登録されたパスワードデータとが一致し、かつ、計測された文字入力間隔と登録された文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に被認証者が本人であると認証する。



【特許請求の範囲】

【請求項 1】 被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力し、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測し、

この入力されたパスワードデータおよび計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合し、

この照合において、前記入力されたパスワードデータおよび計測された文字入力間隔と前記登録されているパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうことを特徴とする個人認証方法。

【請求項 2】 被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力し、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測し、

この入力されたパスワードデータおよび計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合し、

この照合において、前記入力されたパスワードデータと前記登録されているパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記登録されている文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証することを特徴とする個人認証方法。

【請求項 3】 前記パスワードデータの入力時、計時手段により 1 文字ごとの入力時刻を得て、これら得た入力時刻の間で演算を行なうことにより各文字の入力間隔を算出することを特徴とする請求項 1 または 2 記載の個人認証方法。

【請求項 4】 登録時、登録用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

前記入力されたパスワードデータおよび計測された文字入力間隔を登録データとして記憶手段に登録記憶するステップと、

照合時、照合用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

前記入力された照合用のパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、

この照合において、前記入力された照合用のパスワードデータおよび計測された文字入力間隔と前記記憶手段に登録されたパスワードデータおよび文字入力間隔との間

に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうステップと、からなることを特徴とする個人認証方法。

【請求項 5】 登録時、登録用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

文字入力間隔の許容誤差値を入力するステップと、

10 前記入力されたパスワードデータおよび計測された文字入力間隔および入力された許容誤差値を登録データとして記憶手段に登録記憶するステップと、

照合時、照合用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

20 前記入力された照合用のパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、

この照合において、前記入力されたパスワードデータと前記記憶手段に登録されたパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証するステップと、からなることを特徴とする個人認証方法。

【請求項 6】 前記パスワードデータの入力時、計時手段により 1 文字ごとの入力時刻を得て、これら得た入力時刻の間で演算を行なうことにより各文字の入力間隔を算出することを特徴とする請求項 4 または 5 記載の個人認証方法。

【請求項 7】 前記許容誤差値の入力において、許容誤差値の上限値および下限値のうち少なくともいずれか一方を設けることにより、これを超える値の指定を禁止するようにしたことを特徴とする請求項 5 記載の個人認証方法。

【請求項 8】 登録時、被認証者を特定するための識別情報を入力するステップと、

40 登録用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

前記入力された識別情報およびパスワードデータおよび計測された文字入力間隔を登録データとして記憶手段に登録記憶するステップと、

照合時、被認証者を特定するための識別情報を入力するステップと、

照合用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、
前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、
この照合において、前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうステップと、
からなることを特徴とする個人認証方法。

【請求項 9】 登録時、被認証者を特定するための識別情報を入力するステップと、
登録用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、
このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、
文字入力間隔の許容誤差値を入力するステップと、
前記入力された識別情報およびパスワードデータおよび計測された文字入力間隔および入力された許容誤差値を登録データとして記憶手段に登録記憶するステップと、
照合時、被認証者を特定するための識別情報を入力するステップと、
照合用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、
このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、
前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、
この照合において、前記入力された識別情報およびパスワードデータと前記記憶手段に登録された識別情報およびパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証するステップと、
からなることを特徴とする個人認証方法。

【請求項 10】 あらかじめ定められた特定の識別情報が入力された場合に前記文字入力間隔の計測および照合を行なわないようにしたことを特徴とする請求項 8 または 9 記載の個人認証方法。

【請求項 11】 被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するパスワード入力手段と、
このパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する入力間隔計測

手段と、

前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、
この照合手段の照合において、前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔と前記登録されているパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段と、
を具備したことを特徴とする個人認証装置。

【請求項 12】 被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するパスワード入力手段と、

このパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する入力間隔計測手段と、

前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、
この照合手段の照合において、前記パスワード入力手段により入力されたパスワードデータと前記登録されているパスワードデータとの間に所定の関係が成立し、かつ、前記入力間隔計測手段により計測された文字入力間隔と前記登録されている文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段と、
を具備したことを特徴とする個人認証装置。

【請求項 13】 登録時、登録用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力する第 1 のパスワード入力手段と、

この第 1 のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第 1 の入力間隔計測手段と、

前記第 1 のパスワード入力手段により入力されたパスワードデータおよび前記第 1 の入力間隔計測手段により計測された文字入力間隔を登録データとして登録記憶する記憶手段と、

照合時、照合用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力する第 2 のパスワード入力手段と、

この第 2 のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第 2 の入力間隔計測手段と、

前記第 2 のパスワード入力手段により入力された照合用のパスワードデータおよび前記第 2 の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照

合する照合手段と、

この照合手段の照合において、前記第2のパスワード入力手段により入力された照合用のパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録されたパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段と、

を具備したことを特徴とする個人認証装置。

【請求項14】 登録時、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第1のパスワード入力手段と、

この第1のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第1の入力間隔計測手段と、

文字入力間隔の許容誤差値を入力する許容誤差値入力手段と、

前記第1のパスワード入力手段により入力されたパスワードデータおよび前記第1の入力間隔計測手段により計測された文字入力間隔および前記入力間隔計測手段により入力された許容誤差値を登録データとして登録記憶する記憶手段と、

照合時、照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第2のパスワード入力手段と、

この第2のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第2の入力間隔計測手段と、

前記第2のパスワード入力手段により入力された照合用のパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、

この照合手段の照合において、前記第2のパスワード入力手段により入力されたパスワードデータと前記記憶手段に登録されたパスワードデータとの間に所定の関係が成立し、かつ、前記第2の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段と、

を具備したことを特徴とする個人認証装置。

【請求項15】 登録時、被認証者を特定するための識別情報を入力する第1の識別情報入力手段と、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第1のパスワード入力手段と、この第1のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第1の入力間隔計測手段と、

前記第1の識別情報入力手段により入力された識別情報

および前記第1のパスワード入力手段により入力されたパスワードデータおよび前記第1の入力間隔計測手段により計測された文字入力間隔を登録データとして登録記憶する記憶手段と、

照合時、被認証者を特定するための識別情報を入力する第2の識別情報入力手段と、

照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第2のパスワード入力手段と、この第2のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第2の入力間隔計測手段と、

前記第2の識別情報入力手段により入力された照合用の識別情報および前記第2のパスワード入力手段により入力されたパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、

この照合手段の照合において、前記第2の識別情報入力手段により入力された照合用の識別情報および前記第2のパスワード入力手段により入力されたパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段と、

を具備したことを特徴とする個人認証装置。

【請求項16】 登録時、被認証者を特定するための識別情報を入力する第1の識別情報入力手段と、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第1のパスワード入力手段と、この第1のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第1の入力間隔計測手段と、

文字入力間隔の許容誤差値を入力する許容誤差値入力手段と、

前記第1の識別情報入力手段により入力された識別情報および前記第1のパスワード入力手段により入力されたパスワードデータおよび前記第1の入力間隔計測手段により計測された文字入力間隔および前記許容誤差値入力手段により入力された許容誤差値を登録データとして登録記憶する記憶手段と、

照合時、被認証者を特定するための識別情報を入力する第2の識別情報入力手段と、

照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第2のパスワード入力手段と、この第2のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第2の入力間隔計測手段と、

前記第2の識別情報入力手段により入力された照合用の識別情報および前記第2のパスワード入力手段により入

力されたパスワードデータおよび前記第 2 の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、
この照合手段の照合において、前記第 2 の識別情報入力手段により入力された識別情報および前記第 2 のパスワード入力手段により入力されたパスワードデータと前記記憶手段に登録された識別情報およびパスワードデータとの間に所定の関係が成立し、かつ、前記第 2 の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段と、
を具備したことを特徴とする個人認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、たとえば、現金処理機やキャッシュレジスタなどの現金の出入りを管理する端末装置などにおいて、オペレータが使用を許可された者であるか否かの個人認証を行なう個人認証方法および個人認証装置に関する。

【0002】

【従来の技術】たとえば、現金の出入りを管理する現金処理機やキャッシュレジスタ、あるいは、機密情報を保管・表示・操作するパーソナルコンピュータなどの端末装置は、あらかじめ使用を許可された特定のオペレータ（以降、利用者と言うこともある）以外が不正に使用することを防止するため、使用に先立ちパスワードデータのチェックを行なうことが多い。このパスワードデータは、オペレータごとに定められていて、通常は数字や文字もしくはその両者の組み合わせからなる。なお、以降、数字と文字を総称して文字と記す。

【0003】

【発明が解決しようとする課題】ところが、パスワードデータのチェックは、簡便な反面、パスワードデータを盗み見られてしまうと、本人へのなりすましによる不正使用が可能になり、個人認証の精度が著しく低下するという大きな問題がある。

【0004】そこで、本発明は、本人へのなりすましによる不正使用を防止でき、個人認証の精度が著しく向上する個人認証方法および個人認証装置を提供することを目的とする。

【0005】

【課題を解決するための手段】本発明の個人認証方法は、被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力し、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測し、この入力されたパスワードデータおよび計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合し、この照合において、前記入力された

パスワードデータおよび計測された文字入力間隔と前記登録されているパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうことを特徴とする。

【0006】また、本発明の個人認証方法は、被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力し、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測し、この入力されたパスワードデータおよび計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合し、この照合において、前記入力されたパスワードデータと前記登録されているパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記登録されている文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証することを特徴とする。

【0007】また、本発明の個人認証方法は、登録時、登録用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力されたパスワードデータおよび計測された文字入力間隔を登録データとして記憶手段に登録記憶するステップと、照合時、照合用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された照合用のパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、この照合において、前記入力された照合用のパスワードデータおよび計測された文字入力間隔と前記記憶手段に登録されたパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうステップとからなる。

【0008】また、本発明の個人認証方法は、登録時、登録用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、文字入力間隔の許容誤差値を入力するステップと、前記入力されたパスワードデータおよび計測された文字入力間隔および入力された許容誤差値を登録データとして記憶手段に登録記憶するステップと、照合時、照合用の被認証者の複数の文字からなるパスワードデータを 1 文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された照合用のパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、この照合において、前記入力されたパ

スワードデータと前記記憶手段に登録されたパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証するステップとからなる。

【0009】また、本発明の個人認証方法は、登録時、被認証者を特定するための識別情報を入力するステップと、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された識別情報およびパスワードデータおよび計測された文字入力間隔を登録データとして記憶手段に登録記憶するステップと、照合時、被認証者を特定するための識別情報を入力するステップと、照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、この照合において、前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうステップとからなる。

【0010】また、本発明の個人認証方法は、登録時、被認証者を特定するための識別情報を入力するステップと、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、文字入力間隔の許容誤差値を入力するステップと、前記入力された識別情報およびパスワードデータおよび計測された文字入力間隔および入力された許容誤差値を登録データとして記憶手段に登録記憶するステップと、照合時、被認証者を特定するための識別情報を入力するステップと、照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、この照合において、前記入力された識別情報およびパスワードデータと前記記憶手段に登録された識別情報およびパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に

登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証するステップとからなる。

【0011】また、本発明の個人認証装置は、被認証者の複数の文字からなるパスワードデータを1文字ずつ入力するパスワード入力手段と、このパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する入力間隔計測手段と、前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔と前記登録されているパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段とを具備している。

【0012】また、本発明の個人認証装置は、被認証者の複数の文字からなるパスワードデータを1文字ずつ入力するパスワード入力手段と、このパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する入力間隔計測手段と、前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記パスワード入力手段により入力されたパスワードデータと前記登録されているパスワードデータとの間に所定の関係が成立し、かつ、前記入力間隔計測手段により計測された文字入力間隔と前記登録されている文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段とを具備している。

【0013】また、本発明の個人認証装置は、登録時、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第1のパスワード入力手段と、この第1のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第1の入力間隔計測手段と、前記第1のパスワード入力手段により入力されたパスワードデータおよび前記第1の入力間隔計測手段により計測された文字入力間隔を登録データとして登録記憶する記憶手段と、照合時、照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第2のパスワード入力手段と、この第2のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第2の入力間隔計測手段と、前記第2のパスワード入力手段により入力された照合用のパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔と

それぞれ照合する照合手段と、この照合手段の照合において、前記第2のパスワード入力手段により入力された照合用のパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録されたパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段とを具備している。

【0014】また、本発明の個人認証装置は、登録時、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第1のパスワード入力手段と、この第1のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第1の入力間隔計測手段と、文字入力間隔の許容誤差値を入力する許容誤差値入力手段と、前記第1のパスワード入力手段により入力されたパスワードデータおよび前記第1の入力間隔計測手段により計測された文字入力間隔および前記入力間隔計測手段により入力された許容誤差値を登録データとして登録記憶する記憶手段と、照合時、照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第2のパスワード入力手段と、この第2のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第2の入力間隔計測手段と、前記第2のパスワード入力手段により入力された照合用のパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記第2のパスワード入力手段により入力されたパスワードデータと前記記憶手段に登録されたパスワードデータとの間に所定の関係が成立し、かつ、前記第2の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段とを具備している。

【0015】また、本発明の個人認証装置は、登録時、被認証者を特定するための識別情報を入力する第1の識別情報入力手段と、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第1のパスワード入力手段と、この第1のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第1の入力間隔計測手段と、前記第1の識別情報入力手段により入力された識別情報および前記第1のパスワード入力手段により入力されたパスワードデータおよび前記第1の入力間隔計測手段により計測された文字入力間隔を登録データとして登録記憶する記憶手段と、照合時、被認証者を特定するための識別情報を入力する第2の識別情報入力手段と、照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力

する第2のパスワード入力手段と、この第2のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第2の入力間隔計測手段と、前記第2の識別情報入力手段により入力された照合用の識別情報および前記第2のパスワード入力手段により入力されたパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記第2の識別情報入力手段により入力された照合用の識別情報および前記第2のパスワード入力手段により入力されたパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段とを具備している。

【0016】さらに、本発明の個人認証装置は、登録時、被認証者を特定するための識別情報を入力する第1の識別情報入力手段と、登録用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第1のパスワード入力手段と、この第1のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第1の入力間隔計測手段と、文字入力間隔の許容誤差値を入力する許容誤差値入力手段と、前記第1の識別情報入力手段により入力された識別情報および前記第1のパスワード入力手段により入力されたパスワードデータおよび前記第1の入力間隔計測手段により計測された文字入力間隔および前記許容誤差値入力手段により入力された許容誤差値を登録データとして登録記憶する記憶手段と、照合時、被認証者を特定するための識別情報を入力する第2の識別情報入力手段と、照合用の被認証者の複数の文字からなるパスワードデータを1文字ずつ入力する第2のパスワード入力手段と、この第2のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第2の入力間隔計測手段と、前記第2の識別情報入力手段により入力された照合用の識別情報および前記第2のパスワード入力手段により入力されたパスワードデータおよび前記第2の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記第2の識別情報入力手段により入力された識別情報および前記第2のパスワード入力手段により入力されたパスワードデータと前記記憶手段に登録された識別情報およびパスワードデータとの間に所定の関係が成立し、かつ、前記第2の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認

証者が本人であると認証する認証手段とを具備している。

【0017】本発明によれば、被認証者のパスワードデータ入力時における文字入力間隔をあらかじめ登録しておき、被認証者が行なうパスワードデータ入力の際にその文字入力間隔をそれぞれ計測して、あらかじめ登録された文字入力間隔と照合することにより、入力されたパスワードデータおよび計測された文字入力間隔と登録されたパスワードデータおよび文字入力間隔との間に所定の関係が成立するかどうかによって、被認証者が本人であるか否かの認証を行なうことにより、本人へのなりすましによる不正使用を防止でき、個人認証の精度が著しく向上する。

【0018】一般に、パスワードデータが盗み見などにより比較的容易に盗用され易いのに対して、この文字入力間隔は盗み見による盗用がほぼ不可能である。加えて、文字入力間隔の照合を行なっていること自体が極めて発見され難い。この2点から、本発明は極めて破られ難い個人認証方法であると言える。したがって、たとえば、利用許可者以外の操作による端末装置の不正使用を見抜き、かつ、不正使用を防止することができる。

【0019】

【発明の実施の形態】まず、本発明の実施の形態を説明する前に、本発明の概要について簡単に説明しておく。前述したように、たとえば、現金の出入りを管理する現金処理機やキャッシュレジスタ、あるいは、機密情報を保管・表示・操作するパーソナルコンピュータなどの端末装置は、あらかじめ使用を許可された特定のオペレータ以外が不正に使用することを防止するため、使用に先立ちパスワードデータのチェックを行なうことが多い。このパスワードデータは、オペレータごとに定められていて、通常は数字や文字もしくはその両者の組み合わせからなる。

【0020】このような複数の文字から構成されるパスワードデータは、通常、キーボードなどの入力装置から1文字ずつ入力されるが、各文字間の入力間隔時間は、同一のオペレータが同一の文字列を入力する場合には、何度入力を行なってもほぼ同一であるという性質を持つ。言い換えれば、文字入力間隔にはオペレータの癖が出るということで、この性質は特に、同一の文字列入力を行なう回数が増えれば増えるほど強まり、文字入力間隔（時間）の入力ごとのばらつきは少なくなる傾向にある。

【0021】本発明は、このような性質を利用して、パスワードデータの照合に加えて、パスワードデータの文字入力間隔を照合することにより、個人認証の精度を著しく向上するものである。

【0022】以下、本発明の実施の形態について図面を参照して説明する。図1は、本実施の形態に係る個人認証方法および個人認証装置が適用される現金処理機の構

成を概略的に示すものである。本実施の形態に係る現金処理機は、制御手段としてのCPU（セントラル・プロセッシング・ユニット）1、記憶手段としての不揮発性メモリ（たとえば、NVRAM）2、入力手段としてのキーボード3、計時手段としてのタイマ4、および、表示手段としての表示部5、入出金部6、および、通信制御部7から構成されている。

【0023】CPU1は、前記各部をそれぞれ制御したり、データの入出力および演算や比較処理などを行なう。不揮発性メモリ2は、利用者（オペレータ）の従業員番号、パスワードデータ、パスワードデータの文字入力間隔、および、文字入力間隔の許容誤差値を保存（記憶）するパスワード管理エリアを有する。パスワード管理エリアは、たとえば、図2に示すように、従業員番号を記憶する従業員番号保存エリア11、パスワードデータを記憶するパスワード保存エリア12、文字入力間隔を記憶する入力間隔保存エリア13、および、許容誤差値を記憶する許容誤差保存エリア14から構成されている。

【0024】キーボード3は、利用者の現金処理機への操作指示を行なうと共に、利用者を特定する識別情報としての従業員番号、個人認証を行なうためのパスワードデータ、および、パスワードデータの文字入力間隔の許容誤差値などを入力するもので、たとえば、図3に示すように、入金処理を選択する入金キー21、出金処理を選択する出金キー22、および、各種データの入力を行なうテンキー23などが設けられている。

【0025】タイマ4は、時刻情報を生成するもので、CPU1からの指示を受けると、ミリ秒単位で現在の時刻をCPU1に出力する。表示部5は、利用者に対して現金処理機の操作に必要な情報などを表示出力する。

【0026】入出金部6は、入金あるいは出金処理を選択的に行なう。通信制御部7は、図示しないホスト装置との間でオンライン通信を行なう。次に、上記のような構成において、図4および図5に示すフローチャートを参照して、パスワードデータおよびパスワードデータの文字入力間隔を登録する登録処理について説明する。なお、以下に説明する処理は、主にCPU1の制御によって実行される。

【0027】まず、ステップS1にて、図6に示すようなパスワード入力督促画面を表示部5に表示し、たとえば、6桁の従業員番号および4桁のパスワードデータの入力を待機する。ここで、利用者が、まず自己の従業員番号をキーボード3から入力すると（S2）、この入力された従業員番号は、図2に示すように、不揮発性メモリ2のパスワード管理エリア内の従業員番号保存エリア11に格納される（S3）。

【0028】次に、利用者は、従業員番号に続いてパスワードデータの1文字目をキーボード3から入力すると（S4）、このときの時刻t1がタイマ4から読取られ

るとともに (S5)、入力されたパスワードデータの1文字目が、図2に示すように、不揮発性メモリ2のパスワード管理エリア内のパスワード保存エリア12に格納される (S6)。

【0029】次に、利用者は、パスワードデータの2文字目をキーボード3から入力すると (S7)、このときの時刻 t_2 をタイマ4から読取るとともに (S8)、入力されたパスワードデータの2文字目を、図2に示すように、不揮発性メモリ2のパスワード管理エリア内のパスワード保存エリア12に格納する (S9)。

【0030】次に、1文字目の入力時刻 t_1 と2文字目の入力時刻 t_2 との差分 ($t_2 - t_1$) を取ることにより、第1入力間隔 Δt_1 を求め、この求めた第1入力間隔 Δt_1 を、図2に示すように、不揮発性メモリ2のパスワード管理エリア内の入力間隔保存エリア13に格納する (S10)。

【0031】次に、利用者は、パスワードデータの3文字目をキーボード3から入力すると (S11)、このときの時刻 t_3 をタイマ4から読取るとともに (S12)、入力されたパスワードデータの3文字目を、図2に示すように、不揮発性メモリ2のパスワード管理エリア内のパスワード保存エリア12に格納する (S13)。

【0032】次に、2文字目の入力時刻 t_2 と3文字目の入力時刻 t_3 との差分 ($t_3 - t_2$) を取ることにより、第2入力間隔 Δt_2 を求め、この求めた第2入力間隔 Δt_2 を、図2に示すように、不揮発性メモリ2のパスワード管理エリア内の入力間隔保存エリア13に格納する (S14)。

【0033】次に、利用者は、パスワードデータの4文字目をキーボード3から入力すると (S15)、このときの時刻 t_4 をタイマ4から読取るとともに (S16)、入力されたパスワードデータの4文字目を、図2に示すように、不揮発性メモリ2のパスワード管理エリア内のパスワード保存エリア12に格納する (S17)。

【0034】次に、3文字目の入力時刻 t_3 と4文字目の入力時刻 t_4 との差分 ($t_4 - t_3$) を取ることにより、第3入力間隔 Δt_3 を求め、この求めた第3入力間隔 Δt_3 を、図2に示すように、不揮発性メモリ2のパスワード管理エリア内の入力間隔保存エリア13に格納する (S18)。

【0035】次に、図7に示すフローチャートを参照して、パスワードデータの文字入力間隔の許容誤差値を設定 (登録) する第1の設定処理について説明する。なお、以下に説明する処理は、主にCPU1の制御によって実行される。

【0036】まず、ステップS21にて、図9に示すような許容誤差入力督促画面を表示部5に表示し、許容誤差値の入力を待機する。ここで、利用者が所定の許容誤

差値 (%) をキーボード3から入力すると (S22)、この入力された許容誤差値は、図2に示すように、不揮発性メモリ2のパスワード管理エリア内の許容誤差値保存エリア14に格納される (S23)。

【0037】次に、図8に示すフローチャートを参照して、パスワードデータの文字入力間隔の許容誤差値を設定 (登録) する第2の設定処理について説明する。なお、以下に説明する処理は、主にCPU1の制御によって実行される。

10 【0038】この第2の設定処理は、図7に示した基本的な設定処理 (第1の設定処理) に対して、設定値の上限チェックおよび下限チェックを追加している。これは、許容誤差値の設定が大きすぎると、文字入力間隔の照合精度が緩みすぎ、本発明の効果が失われ、許容誤差値の設定が小さすぎると、文字入力間隔の照合精度が厳しくなり過ぎてばらつきを許容できず、不正使用でないのに不正使用と見なしてしまう、という考えに基づいている。

20 【0039】まず、ステップS31にて、図9に示すような許容誤差入力督促画面を表示部5に表示し、許容誤差値の入力を待機する。ここで、利用者が所定の許容誤差値 (%) をキーボード3から入力すると (S32)、この入力された許容誤差値があらかじめ設定される所定の上限値 (たとえば、数値「50」) よりも小さいか否かをチェックする (S33)。

【0040】このチェックの結果、数値「50」よりも小さくなかった場合 (S34)、たとえば、数値「49」を不揮発性メモリ2のパスワード管理エリア内の許容誤差値保存エリア14に格納する (S35)。

30 【0041】ステップS33のチェックの結果、数値「50」よりも小さかった場合 (S34)、入力された許容誤差値があらかじめ設定される所定の下限値 (たとえば、数値「15」) よりも小さいか否かをチェックする (S36)。

【0042】このチェックの結果、数値「15」よりも小さかった場合 (S37)、たとえば、数値「15」を不揮発性メモリ2のパスワード管理エリア内の許容誤差値保存エリア14に格納する (S38)。

40 【0043】ステップS37のチェックの結果、数値「15」よりも小さくなかった場合 (S37)、入力された許容誤差値を不揮発性メモリ2のパスワード管理エリア内の許容誤差値保存エリア14に格納する (S39)。

【0044】次に、図10ないし図13に示すフローチャートを参照して、利用者が利用許可を受けた利用者か否かを調べるためのパスワードデータの照合を行なう照合処理について説明する。なお、以下に説明する処理は、主にCPU1の制御によって実行される。

50 【0045】まず、ステップS41にて、図6に示すようなパスワード入力督促画面を表示部5に表示し、たと

例えば、6桁の従業員番号および4桁のパスワードデータの入力を待機する。ここで、利用者が、まず自己の従業員番号をキーボード3から入力すると（S42）、この入力された従業員番号が不揮発性メモリ2のパスワード管理エリア内の従業員番号保存エリア11に存在するか否かをチェックする（S43）。

【0046】このチェックの結果、入力された従業員番号と同一の従業員番号が従業員番号保存エリア11に存在しなかった場合（S44）、たとえば、図14に示すような利用を拒否する旨の画面（利用拒否画面）を表示部5に表示する（S45、図13参照）。ここで、利用者がその表示を目視して、たとえば、キーボード3でいずれかのキーを押下することにより（S46）、処理を終了する。

【0047】ステップS43のチェックの結果、入力された従業員番号と同一の従業員番号が従業員番号保存エリア11に存在した場合（S44）、入力された従業員番号が特定の番号（たとえば、「999999」）であるか否かをチェックする（S47）。

【0048】このチェックの結果、入力された従業員番号が特定の番号「999999」であった場合（S48）、ステップS49（図13参照）に進む。次に、利用者は、従業員番号に続いてパスワードデータの4文字をキーボード3から入力すると（S49）、この入力されたパスワードデータが不揮発性メモリ2のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア12内のパスワードデータと一致するか否かをチェックする（S50）。

【0049】このチェックの結果、両パスワードデータが一致しなかった場合（S51）、ステップS45に進み、前述同様な動作を繰り返す。ステップS50のチェックの結果、両パスワードデータが一致した場合（S51）、周知の入金処理あるいは出金処理に進む（S52）。

【0050】このように、特定の従業員番号「999999」に対してのみ、パスワードデータの文字入力間隔の照合処理は行なわず、従来と同様なパスワードデータの照合処理だけを行なうものである。

【0051】図10に戻って、ステップS47のチェックの結果、入力された従業員番号が特定の番号「999999」でなかった場合（S48）、ステップS53に進む。次に、利用者は、従業員番号に続いてパスワードデータの1文字目をキーボード3から入力すると（S53）、このときの時刻 t_1 がタイマ4から読取られるとともに（S54）、入力されたパスワードデータの1文字目が、不揮発性メモリ2のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア12内のパスワードデータの1文字目と一致するか否かをチェックする（S55）。

【0052】このチェックの結果、両パスワードデータ

の1文字目が一致しなかった場合（S56）、ステップS45に進み、前述同様な動作を繰り返す。ステップS55のチェックの結果、両パスワードデータの1文字目が一致した場合（S56）、ステップS57に進む。

【0053】次に、利用者は、パスワードデータの2文字目をキーボード3から入力すると（S57）、このときの時刻 t_2 をタイマ4から読取り（S58）、1文字目の入力時刻 t_1 と2文字目の入力時刻 t_2 との差分

$(t_2 - t_1)$ を取ることにより、第1入力間隔 Δt_1 を求め、この求めた第1入力間隔 Δt_1 を、不揮発性メモリ2のパスワード管理エリア内の先に入力された従業員番号に対応する入力間隔保存エリア13内の第1入力間隔 Δt_1 と比較（照合）を行ない、その両者間の誤差が許容誤差値保存エリア13内の許容誤差値の範囲内に収まっているか否かをチェックする（S59）。

【0054】ここで、許容誤差値の範囲内に収まっているための条件式は、以下に示す通りである。

$$-(\text{登録済み許容誤差値}) \leq \{t_{n+1} - t_n\} \div \Delta t_n - 1 \times 100 \geq \text{登録済み許容誤差値} \quad (n=1, 2, 3)$$

ステップS59のチェックの結果、許容誤差値の範囲内に収まっていない場合（S60）、ステップS45に進み、前述同様な動作を繰り返す。ステップS59のチェックの結果、許容誤差値の範囲内に収まっている場合（S60）、入力されたパスワードデータの2文字目が、不揮発性メモリ2のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア12内のパスワードデータの2文字目と一致するか否かをチェックする（S61）。

【0055】このチェックの結果、両パスワードデータの2文字目が一致しなかった場合（S62）、ステップS45に進み、前述同様な動作を繰り返す。ステップS61のチェックの結果、両パスワードデータの2文字目が一致した場合（S62）、ステップS63に進む。

【0056】次に、利用者は、パスワードデータの3文字目をキーボード3から入力すると（S63）、このときの時刻 t_3 をタイマ4から読取り（S64）、2文字目の入力時刻 t_2 と3文字目の入力時刻 t_3 との差分

$(t_3 - t_2)$ を取ることにより、第2入力間隔 Δt_2 を求め、この求めた第2入力間隔 Δt_2 を、不揮発性メモリ2のパスワード管理エリア内の先に入力された従業員番号に対応する入力間隔保存エリア13内の第2入力間隔 Δt_2 と比較（照合）を行ない、その両者間の誤差が許容誤差値保存エリア13内の許容誤差値の範囲内に収まっているか否かをチェックする（S65）。

【0057】このチェックの結果、許容誤差値の範囲内に収まっていない場合（S66）、ステップS45に進み、前述同様な動作を繰り返す。ステップS65のチェックの結果、許容誤差値の範囲内に収まっている場合（S66）、入力されたパスワードデータの3文字目

が、不揮発性メモリ 2 のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア 12 内のパスワードデータの 3 文字目と一致するか否かをチェックする (S67)。

【0058】このチェックの結果、両パスワードデータの 3 文字目が一致しなかった場合 (S68)、ステップ S45 に進み、前述同様な動作を繰り返す。ステップ S67 のチェックの結果、両パスワードデータの 3 文字目が一致した場合 (S68)、ステップ S69 に進む。

【0059】次に、利用者は、パスワードデータの 4 文字目をキーボード 3 から入力すると (S69)、このときの時刻 t_4 をタイマ 4 から読取り (S70)、3 文字目の入力時刻 t_3 と 4 文字目の入力時刻 t_4 との差分

($t_4 - t_3$) を取ることにより、第 3 入力間隔 Δt_3 を求め、この求めた第 3 入力間隔 Δt_3 を、不揮発性メモリ 2 のパスワード管理エリア内の先に入力された従業員番号に対応する入力間隔保存エリア 13 内の第 3 入力間隔 Δt_3 と比較 (照合) を行ない、その両者間の誤差が許容誤差値保存エリア 13 内の許容誤差値の範囲内に収まっているか否かをチェックする (S71)。

【0060】このチェックの結果、許容誤差値の範囲内に収まっていない場合 (S72)、ステップ S45 に進み、前述同様な動作を繰り返す。ステップ S71 のチェックの結果、許容誤差値の範囲内に収まっている場合

(S72)、入力されたパスワードデータの 4 文字目が、不揮発性メモリ 2 のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア 12 内のパスワードデータの 4 文字目と一致するか否かをチェックする (S73)。

【0061】このチェックの結果、両パスワードデータの 4 文字目が一致しなかった場合 (S74)、ステップ S45 に進み、前述同様な動作を繰り返す。ステップ S73 のチェックの結果、両パスワードデータの 4 文字目が一致した場合 (S74)、周知の入金処理あるいは出金処理に進む (S52)。

【0062】このように、まず、利用者を特定するために従業員番号の入力を利用者に求め、従業員番号が登録されたものであるか否かをチェックし、利用者を特定する。これ以降、パスワードデータの文字入力ごとにタイマ 4 から時刻を読出し、それぞれの差分をとることにより文字の入力間隔を求める。求めた文字入力間隔をあらかじめ登録済みの入力間隔とそれぞれ比較し、両者間の誤差があらかじめ登録済みの許容誤差値の範囲内に収まっているか否かをチェックする。これと同時に、入力されたパスワードデータが正しいものか否かのチェックを文字入力ごとに行なう。これらの各チェックを全てパスした場合にのみ、利用者 (オペレータ) は本人であると認証して、入金処理あるいは出金処理を許可し、パスしなかった場合には、利用者は本人でないと認証して、利用を拒否する旨の画面を表示部 5 に表示し、入金処理あ

るいは出金処理は行なわない。

【0063】以上説明したように、上記実施の形態によれば、利用者のパスワードデータの入力時における文字の入力間隔をあらかじめ登録しておき、利用者が現金処理機の利用に先立って行なうパスワードデータ入力の際に文字の入力間隔 (時間) を計測して、両者を照合し、同一人物と認められた場合にのみ、現金処理機の利用を許可することにより、利用許可者以外の操作による現金処理機的不正使用を見抜ねき、かつ、不正使用を防止することができる。

【0064】パスワードデータが盗み見などにより比較的容易に盗用され易いのに対して、この文字入力間隔は盗み見による盗用がほぼ不可能である。加えて、文字入力間隔の照合を行なっていること自体が極めて発見され難い。これらから、本発明は極めて破られ難い個人認証方法であると言える。

【0065】利用者を特定するための識別情報 (実施の形態では従業員番号だが、他に氏名なども考えられる) の入力に際しても、本発明の文字入力間隔照合を施すことにより、個人認証の精度がさらに向上する。

【0066】特定の従業員番号 (実施の形態では「99999999」) に対して、選択的に文字入力間隔の照合処理を施さない手段を設け、この従業員番号とパスワードデータを管理者用に割り当て、管理者のみに公開することにより、複数の管理者による機器の運用管理が可能になる。

【0067】許容誤差値の入力において、許容誤差値の最大値 (実施の形態では 49%) を設け、これを超える指定を禁止する手段を設けることにより、文字入力間隔の照合精度が落ち過ぎて本発明の効果が失われることを防止できる。

【0068】許容誤差値の入力において、許容誤差値の最小値 (実施の形態では 15%) を設け、これを下回る値の指定を禁止する手段を設けることにより、文字入力間隔の照合精度を上げ過ぎて不正使用でないにも拘らず、照合をパスできなくなることを防止できる。

【0069】

【発明の効果】以上詳述したように本発明よれば、本人へのなりすましによる不正使用を防止でき、個人認証の精度が著しく向上する個人認証方法および個人認証装置を提供できる。

【図面の簡単な説明】

【図 1】本発明の実施の形態に係る個人認証方法および個人認証装置が適用される現金処理機の構成を概略的に示すブロック図。

【図 2】不揮発性メモリ内のパスワード管理エリアを説明する構成図。

【図 3】キーボードの構成を示す平面図。

【図 4】パスワードデータおよびパスワードデータの文字入力間隔を登録する登録処理を説明するフローチャー

ト。

【図 5】パスワードデータおよびパスワードデータの文字入力間隔を登録する登録処理を説明するフローチャート。

【図 6】パスワード入力督促画面の一例を示す平面図。

【図 7】パスワードデータの文字入力間隔の許容誤差値を設定する第 1 の設定処理を説明するフローチャート。

【図 8】パスワードデータの文字入力間隔の許容誤差値を設定する第 2 の設定処理を説明するフローチャート。

【図 9】許容誤差入力督促画面の一例を示す平面図。

【図 10】パスワードデータの照合を行なう照合処理を説明するフローチャート。

【図 11】パスワードデータの照合を行なう照合処理を

説明するフローチャート。

【図 12】パスワードデータの照合を行なう照合処理を説明するフローチャート。

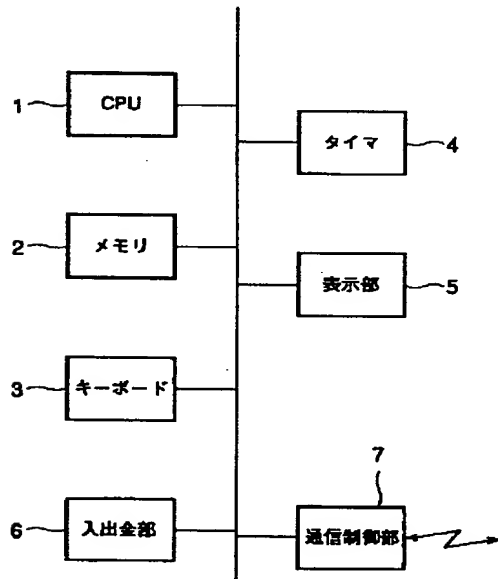
【図 13】パスワードデータの照合を行なう照合処理を説明するフローチャート。

【図 14】利用拒否画面の一例を示す平面図。

【符号の説明】

1……CPU、2……不揮発性メモリ、3……キーボード、4……タイマ、5……表示部、6……入出金部、7……通信制御部、11……従業員番号保存エリア、12……パスワード保存エリア、13……入力間隔保存エリア、14……許容誤差保存エリア。

【図 1】



【図 6】

テンキーから従業員番号とパスワードを入力して下さい。

従業員番号

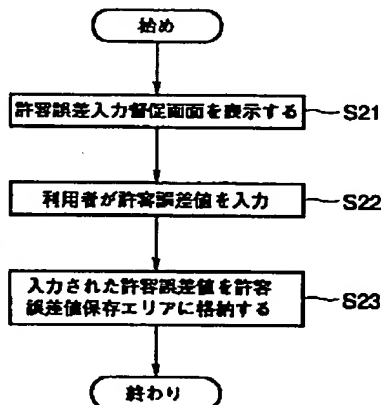
パスワード

【図 2】

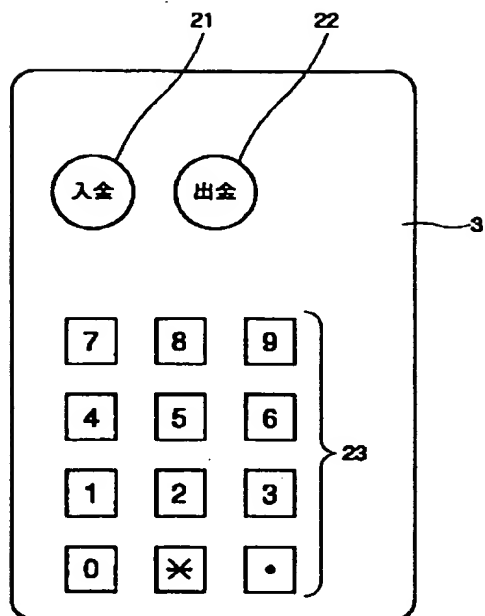
従業員番号	パスワードデータ	文字入力間隔 (m sec)			許容誤差 (%)
		Δt1	Δt2	Δt3	
8 2 0 4 5 8	5 1 2 6	1363	1046	521	49
7 5 1 0 9 9	0 8 1 2	358	312	407	40
7 1 1 4 1 5	0 4 6 5	267	325	929	35
8 7 0 2 7 8	1 3 8 1	443	962	287	30
8 8 0 8 4 8	1 9 5 9	1172	473	821	15
9 9 9 9 9 9	1 1 2 9	0	0	0	0

11
12
13
14

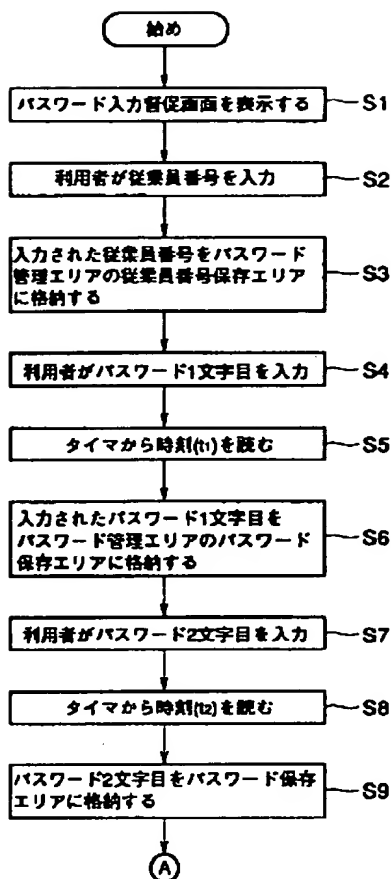
【図 7】



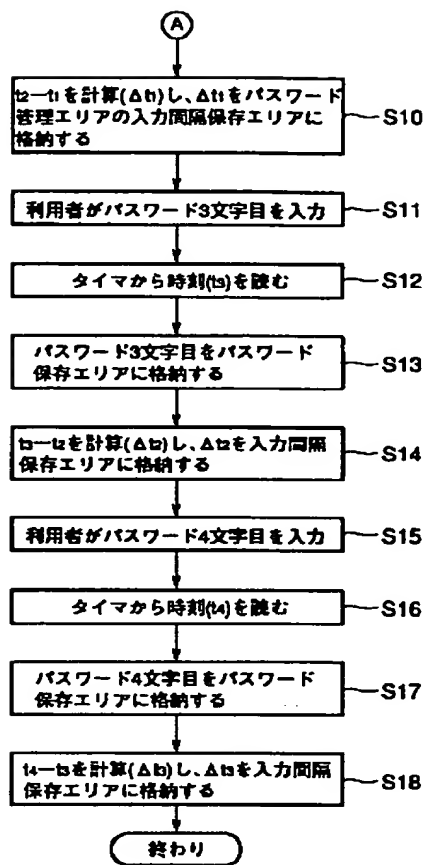
【図 3】



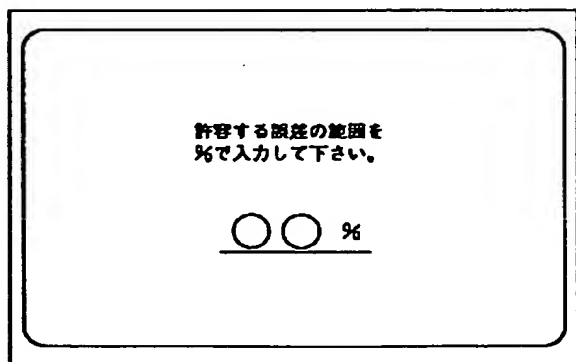
【図 4】



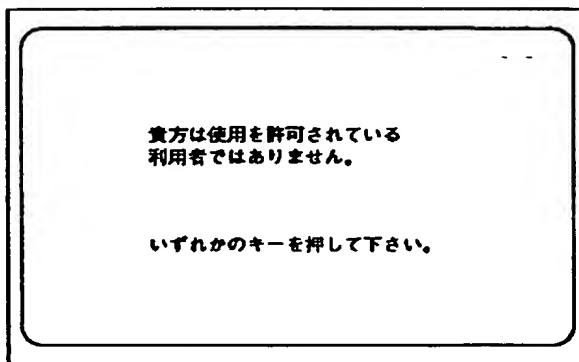
【図 5】



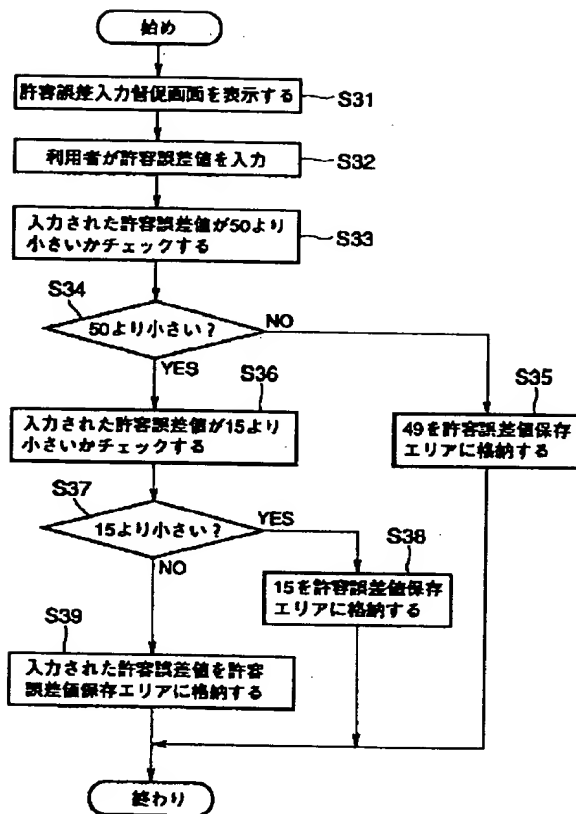
【図 9】



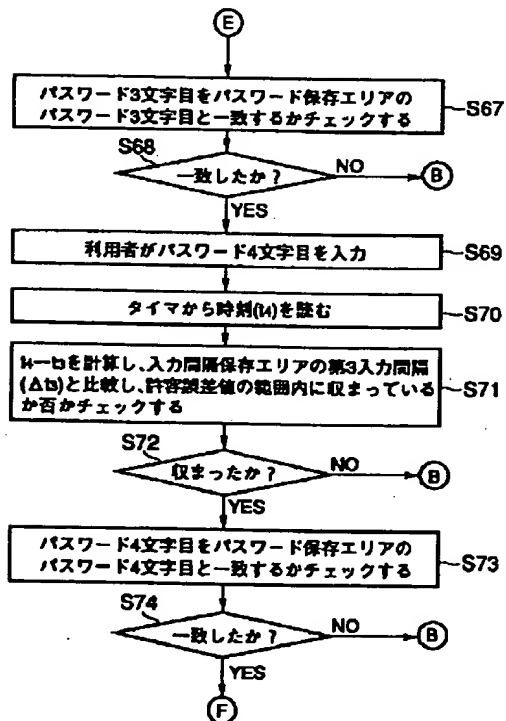
【図 14】



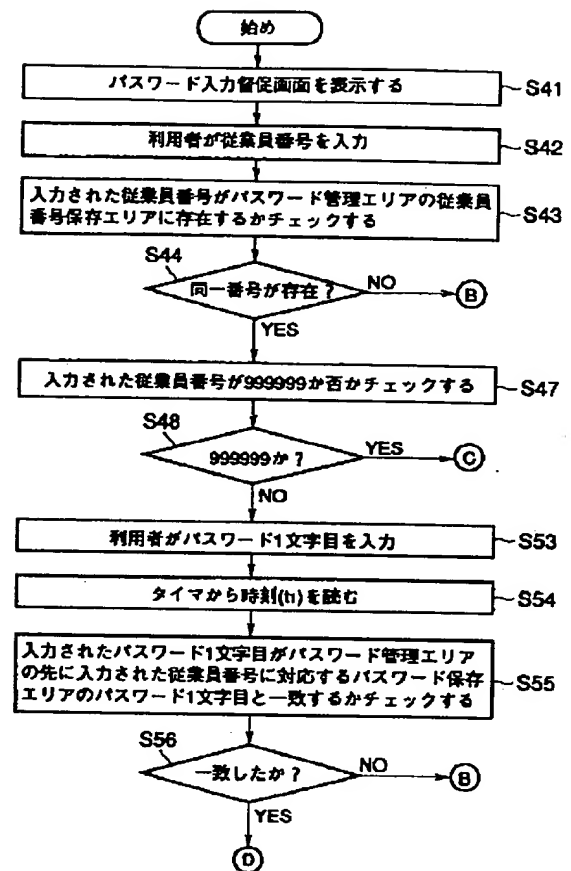
【図8】



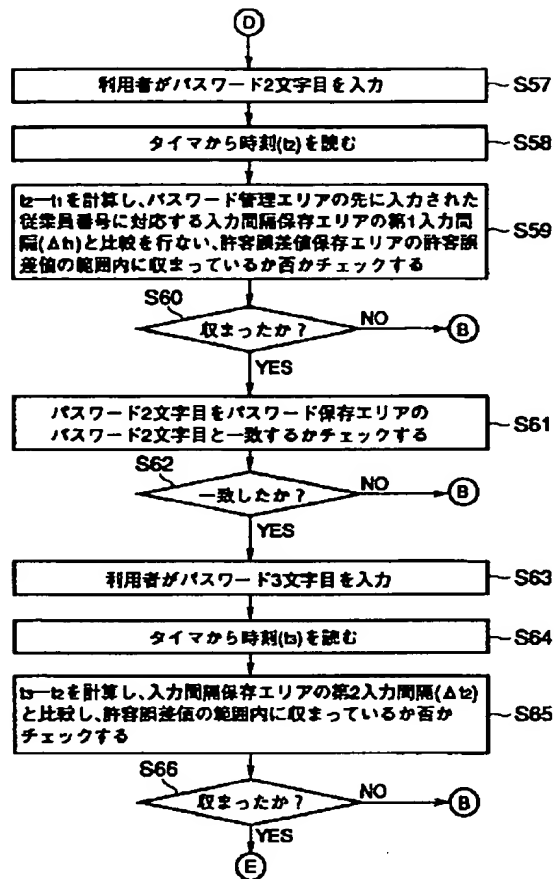
【図12】



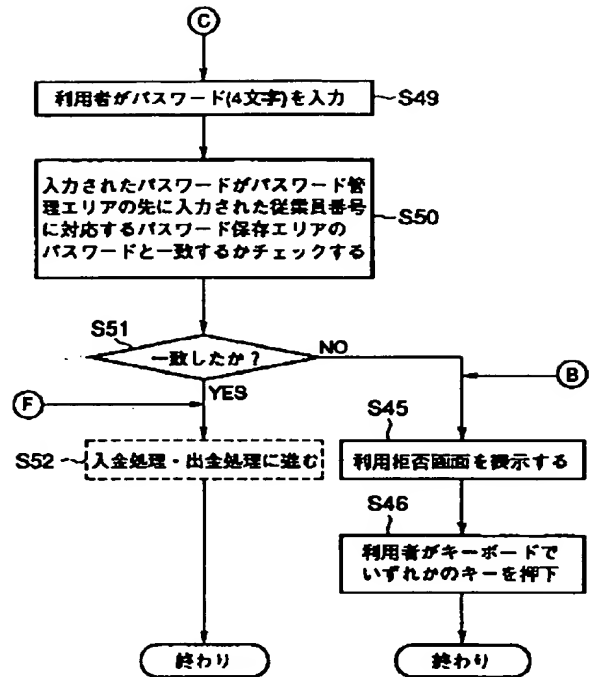
【図10】



【図11】



【図13】



THIS PAGE BLANK (USPTO)